明細書

サービス不能攻撃検知システムおよびサービス不能攻撃検知方法

技術分野

[0001] この発明は、サービス不能攻撃対象となる通信機器宛に送信されたパケットを監視する監視装置と、この通信機器の性能を測定する性能測定装置と、監視装置および性能測定装置と通信をおこなう攻撃判断装置とによってかかる通信機器に対するサービス不能攻撃を検知するサービス不能攻撃検知システムおよびサービス不能攻撃検知方法に関し、特に、サービス不能攻撃の検知精度を向上させることにより対処の必要なサービス不能攻撃のみを検知することができるサービス不能攻撃検知システムおよびサービス不能攻撃検知方法に関する。

背景技術

[0002] 従来、ネットワークを介した攻撃として、多量のパケットを送付することによりネットワークやサーバマシン（以下「通信機器」と言う）を麻痺させるサービス不能攻撃（分散型サービス不能攻撃を含む）が知られている。かかるサービス不能攻撃は、パケットの特徴量を用いた方法では検知しにくいことから、トラフィック（量）の異常性を用いた方法によるサービス不能攻撃検知システムが広く用いられている。

[0003] このサービス不能攻撃検知システムは、攻撃対象となる通信機器宛のトラフィックを所定の期間にわたって測定することにより求められる定常トラフィックを、手動または自動であらかじめ算出する。そして、監視しているトラフィックが、かかる定常トラフィックから乖離した場合に攻撃とみなすこととして、サービス不能攻撃を検知している（例えば、特許文献1参照）。

[0004] 特許文献1：特開2004－283555号公報

発明の開示

発明が解決しようとする課題

[0005] しかしながら、かかるサービス不能攻撃においては、攻撃規模と、ネットワークおよび通信機器の処理能力との関係から、トラフィックが異常性を示したとしても通信機器が提供するサービスに実害がない場合が多々存在する。このような場合には、上述し

たサービス不能攻撃検知システムが攻撃として検知しても、具体的な対処を行う必要がないために、誤検知したことと何らかわりがないことになってしまう。

[0006] サービス不能攻撃検知システムの主たる用途が通信機器をサービス不能にする攻撃から防御することであるとの考えに基づけば、トラフィックの異常性が攻撃であるか否かを見極める精度を向上させることより、パフォーマンスの劣化を引き起こしているトラフィックの異常性を早急に見つけることが重要である。しかし、従来のサービス不能攻撃検知システムでは、通信機器の処理能力等を考慮することなく、トラフィックの異常性のみに基づいて攻撃を検知しようとしており、パフォーマンスの劣化と関連のないトラフィックの異常性の検知、言い換えれば、対処の必要がない状況の検知(広い意味での誤検知)が多くなるれづ課題があった。

[0007] 本発明は、上述した従来技術による問題点を解消するためになされたものであり、サービス不能攻撃の検知精度を向上させることにより対処を必要とするサービス不能攻撃のみを検知することができるサービス不能攻撃検知システムおよびサービス不能攻撃検知方法を提供することを目的とする。

課題を解決するための手段

[0008] 上述した課題を解決し、目的を達成するため、本発明は、サービス不能攻撃対象となる通信機器宛に送信されたパケットを監視する監視装置と、前記通信機器の性能を測定する性能測定装置と、前記監視装置および前記性能測定装置と通信をおこなう攻撃判断装置とによって前記通信機器に対するサービス不能攻撃を検知するサービス不能攻撃検知システムであって、前記監視装置は、前記通信機器に対する前記パケットによるトラフィックの異常性を表すトラフィック異常性情報を検知するトラフィック異常性検知手段を備え、前記性能測定装置は、前記通信機器の処理能力の異常性を表す性能異常性情報を検知する性能異常性検知手段を備え、前記攻撃判断装置は、前記トラフィック異常性情報および前記性能異常性情報に基づいてサービス不能攻撃であるか否かを判断する影響判断手段を備えたことを特徴とする。

[0009] この発明によれば、監視装置が通信機器に対するパケットによるトラフィックの異常性を表すトラフィック異常性情報を検知し、性能測定装置が通信機器の処理能力の異常性を表す性能異常性情報を検知し、攻撃判断装置がトラフィック異常性情報お

よび性能異常性情報に基づいてサービス不能攻撃であるか否かを判断することとしたので、トラフィック異常性情報のみならず性能異常性情報を用いてこれらの異常性情報の関連によってサービス不能攻撃であるか否かを判断することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0010] また、本発明は、上記発明において、前記監視装置は、前記トラフィック異常性情報を前記攻撃判断装置に送信するトラフィック異常性情報送信手段をさらに備えたことを特徴とする。

[0011] この発明によれば、監視装置がトラフィック異常性情報を攻撃判断装置に送信することとしたので、攻撃判断装置が監視装置のトラフィック異常性情報を参照することなくトラフィック異常性情報を効率的に取得することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0012] また、本発明は、上記発明において、前記性能測定装置は、前記性能異常性情報を前記攻撃判断装置に送信する性能異常性情報送信手段をさらに備えたことを特徴とする。

[0013] この発明によれば、性能測定装置が性能異常性情報を攻撃判断装置に送信することとしたので、攻撃判断装置が性能測定装置の性能異常性情報を参照することなく性能異常性情報を効率的に取得することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0014] また、本発明は、上記発明において、前記トラフィック異常性検知手段は、あらかじめ設定された所定の攻撃検知条件に基づいて前記トラフィック異常性情報を検知することを特徴とする。

[0015] この発明によれば、あらかじめ設定された所定の攻撃検知条件に基づいてトラフィック異常性情報を検知することとしたので、監視装置が効率的にトラフィック異常性情報を検知することができるとともに、攻撃検知条件を変更することにより、攻撃パターンが異なるあらたな攻撃に容易に対処することができる。

[0016] また、本発明は、上記発明において、前記トラフィック異常性検知手段は、前記攻撃検知条件に基づいて前記通信機器に対する攻撃をおこなうパケットの特徴を表す

シグネチャを生成し、前記シグネチャを含む前記トラフィック異常性情報を生成することを特徴とする。

[0017] この発明によれば、攻撃検知条件に基づいて通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを生成し、かかるシグネチャを含むトラフィック異常性情報を生成することとしたので、攻撃をおこなうパケットの特徴を反映したトラフィック異常性情報を生成することにより、トラフィック異常性情報の信頼性を向上させることができる。

[0018] また、本発明は、上記発明において、前記トラフィック異常性検知手段は、前記通信機器宛の前記パケットの平均的なトラフィックを表す定常トラフィックに基づいて前記トラフィック異常性情報を検知することを特徴とする。

[0019] この発明によれば、通信機器宛のパケットの平均的なトラフィックを表す定常トラフィックに基づいてトラフィック異常性情報を検知することとしたので、検知されたトラフィックと定常トラフィックとの乖離状況に基づいて簡便にトラフィック異常性情報を生成することができる。

[0020] また、本発明は、上記発明において、前記性能異常性検知手段は、あらかじめ設定された所定の性能異常性検知条件に基づいて前記性能異常性情報を検知することを特徴とする。

[0021] この発明によれば、あらかじめ設定された所定の性能異常性検知条件に基づいて性能異常性情報を検知することとしたので、性能測定装置が効率的に性能異常性情報を検知することができるとともに、性能異常性検知条件を変更することにより、検知対象となる通信機器の性能の差異や性能の変化に容易に対処することができる。

[0022] また、本発明は、上記発明において、前記性能異常性検知条件は、前記通信機器に応答要求メッセージを送信してから前記応答要求メッセージに対応する応答メッセージを受信するまでの応答時間と、前記応答時間が所定の閾値を上回る回数とを含んだことを特徴とする。

[0023] この発明によれば、通信機器に応答要求メッセージを送信してから応答要求メッセージに対応する応答メッセージを受信するまでの応答時間と、応答時間が所定の閾値を上回る回数とを含むこととしたので、通信機器の応答時間に基づいて簡便に性

能異常性情報を生成することができる。

[0024] また、本発明は、上記発明において、前記性能異常性検知手段は、前記通信機器の平均的な性能特性を表す定常性能に基づいて前記性能異常性情報を検知することを特徴とする。

[0025] この発明によれば、通信機器の平均的な性能特性を表す定常性能に基づいて性能異常性情報を検知することとしたので、検知された性能と定常性能特性との乖離状況に基づいて簡便に性能異常性情報を生成することができる。

[0026] また、本発明は、上記発明において、前記攻撃判断手段は、前記トラフィック異常性情報および前記性能異常性情報に含まれる異常発生時刻に基づいて該トラフィック異常性情報または該性能異常性情報のいずれか一方の異常性情報に起因して他方の異常性情報が発生したと判断した場合にサービス不能攻撃であると判断することを特徴とする。

[0027] この発明によれば、トラフィック異常性情報および性能異常性情報に含まれる異常発生時刻に基づいてトラフィック異常性情報または性能異常性情報のいずれか一方の異常性情報に起因して他方の異常性情報が発生したと判断した場合にサービス不能攻撃であると判断することとしたので、トラフィック異常性情報のみならず性能異常性情報を用いてこれらの異常性情報の関連によってサービス不能攻撃であるか否かを判断することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0028] また、本発明は、上記発明において、前記影響判断手段がサービス不能攻撃であると判断した場合に、該判断に用いた前記トラフィック異常性情報および前記性能異常性情報を前記攻撃判断装置がオペレータ通知用装置に送信することを特徴とする。

[0029] この発明によれば、攻撃判断装置がサービス不能攻撃であると判断した場合に、判断に用いたトラフィック異常性情報および性能異常性情報をオペレータ通知用装置に送信することとしたので、これらの性能異常性情報に基づいてオペレータが適切な対処をすることができる。

[0030] また、本発明は、上記発明において、前記影響判断手段は、前記トラフィック異常

性情報および前記性能異常性情報に含まれる証明書に基づいた認証を行ったうえで、サービス不能攻撃であるか否かを判断することを特徴とする。

[0031] この発明によれば、トラフィック異常性情報および性能異常性情報に含まれる証明書に基づいた認証を行ったうえで、サービス不能攻撃であるか否かを判断することとしたので、非正規な装置を用いたなりすましを効果的に防止することができる。

[0032] また、本発明は、サービス不能攻撃対象となる通信機器宛に送信されたパケットを監視する監視装置と、前記通信機器の性能を測定する性能測定装置と、前記監視装置および前記性能測定装置と通信をおこなう攻撃判断装置とによって前記通信機器に対するサービス不能攻撃を検知するサービス不能攻撃検知方法であって、前記通信機器に対する前記パケットによるトラフィックの異常性を表すトラフィック異常性情報を前記監視装置が検知するトラフィック異常性検知工程と、前記通信機器の処理能力の異常性を表す性能異常性情報を前記性能測定装置が検知する性能異常性検知工程と、前記トラフィック異常性情報および前記性能異常性情報に基づいてサービス不能攻撃であるか否かを前記攻撃判断装置が判断する影響判断工程とを含んだことを特徴とする。

[0033] この発明によれば、監視装置が通信機器に対するパケットによるトラフィックの異常性を表すトラフィック異常性情報を検知し、性能測定装置が通信機器の処理能力の異常性を表す性能異常性情報を検知し、攻撃判断装置がトラフィック異常性情報および性能異常性情報に基づいてサービス不能攻撃であるか否かを判断することとしたので、トラフィック異常性情報のみならず性能異常性情報を用いてこれらの異常性情報の関連によりサービス不能攻撃であるか否かを判断することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0034] また、本発明は、上記発明において、前記トラフィック異常性情報を前記監視装置が前記攻撃判断装置に送信するトラフィック異常性情報送信工程をさらに含んだことを特徴とする。

[0035] この発明によれば、監視装置がトラフィック異常性情報を攻撃判断装置に送信することとしたので、攻撃判断装置が監視装置のトラフィック異常性情報を参照することな

くトラフィック異常性情報を効率的に取得することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0036] また、本発明は、上記発明において、前記性能異常性情報を前記性能測定装置が前記攻撃判断装置に送信する性能異常性情報送信工程をさらに含んだことを特徴とする。

[0037] この発明によれば、性能測定装置が性能異常性情報を攻撃判断装置に送信することとしたので、攻撃判断装置が性能測定装置の性能異常性情報を参照することなく性能異常性情報を効率的に取得することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

発明の効果

[0038] 本発明によれば、監視装置が通信機器に対するパケットによるトラフィックの異常性を表すトラフィック異常性情報を検知し、性能測定装置が通信機器の処理能力の異常性を表す性能異常性情報を検知し、攻撃判断装置がトラフィック異常性情報および性能異常性情報に基づいてサービス不能攻撃であるか否かを判断することとしたので、トラフィック異常性情報のみならず性能異常性情報を用いてこれらの異常性情報の関連によってサービス不能攻撃であるか否かを判断することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0039] また、本発明によれば、監視装置がトラフィック異常性情報を攻撃判断装置に送信することとしたので、攻撃判断装置が監視装置のトラフィック異常性情報を参照することなくトラフィック異常性情報を効率的に取得することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0040] また、本発明によれば、性能測定装置が性能異常性情報を攻撃判断装置に送信することとしたので、攻撃判断装置が性能測定装置の性能異常性情報を参照することなく性能異常性情報を効率的に取得することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0041] また、本発明によれば、あらかじめ設定された所定の攻撃検知条件に基づいてトラフィック異常性情報を検知することとしたので、監視装置が効率的にトラフィック異常

性情報を検知することができるとともに、攻撃検知条件を変更することにより、攻撃パターンが異なるあらたな攻撃に容易に対処することができる。

[0042] また、本発明によれば、攻撃検知条件に基づいて通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを生成し、かかるシグネチャを含むトラフィック異常性情報を生成することとしたので、攻撃をおこなうパケットの特徴を反映したトラフィック異常性情報を生成することにより、トラフィック異常性情報の信頼性を向上させることができる。

[0043] また、本発明によれば、通信機器宛のパケットの平均的なトラフィックを表す定常トラフィックに基づいてトラフィック異常性情報を検知することとしたので、検知されたトラフィックと定常トラフィックとの乖離状況に基づいて簡便にトラフィック異常性情報を生成することができる。

[0044] また、本発明によれば、あらかじめ設定された所定の性能異常性検知条件に基づいて性能異常性情報を検知することとしたので、性能測定装置が効率的に性能異常性情報を検知することができるとともに、性能異常性検知条件を変更することにより、検知対象となる通信機器の性能の差異や性能の変化に容易に対処することができる。

[0045] また、本発明によれば、通信機器に応答要求メッセージを送信してから応答要求メッセージに対応する応答メッセージを受信するまでの応答時間と、応答時間が所定の閾値を上回る回数とを含むこととしたので、通信機器の応答時間に基づいて簡便に性能異常性情報を生成することができる。

[0046] また、本発明によれば、通信機器の平均的な性能特性を表す定常性能に基づいて性能異常性情報を検知することとしたので、検知された性能と定常性能との乖離状況に基づいて簡便に性能異常性情報を生成することができる。

[0047] また、本発明によれば、トラフィック異常性情報および性能異常性情報に含まれる異常発生時刻に基づいてトラフィック異常性情報または性能異常性情報のいずれか一方の異常性情報に起因して他方の異常性情報が発生したと判断した場合にサービス不能攻撃であると判断することとしたので、トラフィック異常性情報のみならず性能異常性情報を用いてこれらの異常性情報の関連によりサービス不能攻撃であるか

否かを判断することにより、サービス不能攻撃の検知精度を向上させ対処の必要なサービス不能攻撃のみを検知することができる。

[0048] また、本発明によれば、攻撃判断装置がサービス不能攻撃であると判断した場合に、判断に用いたトラフィック異常性情報および性能異常性情報をオペレータ通知用装置に送信することとしたので、これらの性能異常性情報に基づいてオペレータが適切な対処をすることができる。

[0049] また、本発明によれば、トラフィック異常性情報および性能異常性情報に含まれる証明書に基づいた認証を行ったうえで、サービス不能攻撃であるか否かを判断することとしたので、非正規な装置を用いたなりすましを効果的に防止することができる。

図面の簡単な説明

[0050] [図1]図1は、本実施例に係るサービス不能攻撃検知システムの構成を示すブロック図である。

[図2]図2は、図1に示した監視装置の構成を示すブロック図である。

[図3]図3は、攻撃検知条件の一例を示す図である。

[図4]図4は、図1に示した性能測定装置の構成を示すブロック図である。

[図5]図5は、性能異常性検知条件の一例を示す図である。

[図6]図6は、図1に示した攻撃判断装置の構成を示すブロック図である。

[図7]図7は、図2に示した監視装置の動作を示すフローチャートである。

[図8]図8は、図4に示した性能測定装置の動作を示すフローチャートである。

[図9]図9は、図6に示した攻撃判断装置の動作を示すフローチャートである。

符号の説明

[0051] 1 サービス不能攻撃検知システム

2 LAN

3 通信機器

4 WAN

5 監視装置

6、9 通信回線

7 性能測定装置

8 攻撃判断装置

10 トラフィック異常性検知部

11 トラフィック異常性情報送信部

12 シグネチャ生成部

13、14、18、19、22 通信インタフェイス

15 スイッチ

16 性能異常性検知部

17 性能異常性情報送信部

20 影響判断部

21 アラート送信部

発明を実施するための最良の形態

[0052] 以下に添付図面を参照して、この発明に係るサービス不能攻撃検知システムおよびサービス不能攻撃検知方法の好適な実施の形態を詳細に説明する。

実施例

[0053] 図1は、本実施例に係るサービス不能攻撃検知システム1の構成を示すブロック図である。同図に示すサービス不能攻撃検知システム1は、通信機器3へのサービス不能攻撃を監視装置5、性能測定装置7および攻撃判断装置8を用いて検知するシステムである。具体的には、LAN(Local Area Network)2上の監視装置5が通信機器3宛のパケットによるトラフィック異常を検知したならば(図1のステップ1)、かかるトラフィック異常の内容を表すトラフィック異常性情報を攻撃判断装置8に送信する(図1のステップ2)。

[0054] また、WAN(Wide Area Network)4上の性能測定装置7が通信機器3の性能異常を検知したならば(図1のステップ3)、かかる性能異常の内容を表す性能異常性情報を攻撃判断装置8に送信する(図1のステップ4)。そして、LAN2上の攻撃判断装置8がトラフィック異常性情報および性能異常性情報を受信したならば、これらの異常性情報に基づいて通信機器3に対するサービス不能攻撃であるか否かを判断する(図1のステップ5)こととしている。

[0055] 従来、通信機器3を攻撃対象とするサービス不能攻撃を検知する場合には、攻撃

対象となる通信機器3宛のトラフィックを所定の期間にわたって測定することにより定常トラフィックをあらかじめ算出し、監視しているトラフィックが、かかる定常トラフィックから乖離した場合に攻撃とみなすこととしてサービス不能攻撃を検知していた。しかしながら、サービス不能攻撃の攻撃規模と、ネットワークおよび通信機器の処理能力との関係から、トラフィックが異常性を示したとしても通信機器3が提供するサービスに実害がない場合が多々存在した。このため、サービス不能攻撃として検知された場合であっても、実際には何ら対処の必要がないことも多く、実質的に誤検知したことと何らかわりがない状況が発生していた。

[0056] 本実施例では、トラフィック異常性の検知を監視装置5が行い、通信装置3の性能異常性の検知を性能測定装置7が行うこととし、さらに、トラフィック異常性および性能異常性に基づいた攻撃判断を攻撃判断装置8が行うこととしている。したがって、本実施例によれば、トラフィック異常性のみならず通信機器3の性能異常性に基づいた攻撃判断をすることができるので、サービス不能攻撃の検知精度向上により、対処を必要とするサービス不能攻撃のみを効果的に検知することができる。

[0057] なお、図1においては、監視装置5および攻撃判断装置8が通信機器3と同一のLAN2に接続され、性能測定装置7がWAN4に接続された場合について図示しているが、各装置(監視装置5、性能測定装置7および攻撃判断装置8)が接続される回線を限定するものではない。

[0058] 次に、このサービス不能攻撃検知システム1のシステム構成について説明する。図1に示すように、このサービス不能攻撃検知システム1は、中小企業内のLAN2に設けられ、LAN2に接続された少なくとも1つの通信機器3に基幹回線網等のWAN4を介して送信されたパケットを監視する監視装置5と、WAN4に設けられ、WAN4を介して通信機器3の性能を測定する性能測定装置7と、LAN2に設けられ、監視装置5および性能測定装置7と通信回線9により接続された攻撃判断装置8とを備えている。なお、図1に示したサービス不能攻撃検知システム1の構成は一例を示すものであり、本発明のサービス不能攻撃検知システムは、複数の性能測定装置7を備えてもよく、これらの性能測定装置6の一部またはすべてを、他者が提供するWeb (WorldWideWeb)サイト性能測定サービスを使うように構成してもよい。

[0059] 監視装置5は、LAN2を構成するルータによって構成されている。なお、監視装置5は、LAN2に設けられたファイアウォール等によって構成してもよい。

[0060] 図2は、図1に示した監視装置5の構成を示すブロック図である。監視装置5は、通信機器3に送信されるパケットによるトラフィックの異常性を検知するトラフィック異常性検知部10と、検知したトラフィック異常性情報を攻撃判断装置8に送信するトラフィック異常性情報送信部11と、通信機器3に対する攻撃を行うパケットの特徴を表すシグネチャを生成するシグネチャ生成部12と、WAN4およびLAN2に設けられた攻撃判断装置8を含む各装置とそれぞれ通信を行うための通信インタフェイス13、14と、パケットをルーティングするためのスイッチ15とを備えている。

[0061] トラフィック異常性検知部10は、あらかじめ設定された攻撃検知条件に基づいて攻撃を検知する処理部である。図3は、攻撃検知条件の一例を示す図である。図3において、攻撃検知条件は、検知属性、検知閾値および検知時間の組からなる2組のレコードで構成される。検知属性は、検知対象とするパケットの属性を示し、検知閾値は、検知対象となるパケットの伝送レートの閾値を示し、検知時間は、検知対象となるパケットの伝送レートが検知閾値を超える時間の閾値を示している。

[0062] 例えば、1番目の検知条件は、宛先のアドレス情報が192.168.1.1であり(Dst=192.168.1.1/32)、トランスポート層のプロトコルがTCP(TransmissionControlProtocol)であり(Protocol=TCP)、TCPポート番号が80である(Port=80パケットが検知対象となり、この検知対象のパケットの伝送レートが300kbpsを超えた状態が10秒以上続いた場合には、検知対象のパケットによるトラフィック異常性として検知される。

[0063] 同様に、2番目の検知条件は、宛先のアドレス情報が192.168.1.2(Dst=192.168.1.2/32)であるパケットが検知対象となり、この検知対象のパケットの伝送レートが100kbpsを超えた状態が10秒以上続いた場合には、検知対象のパケットによるトラフィック異常性として検知される。

[0064] このように、検知対象のパケットによる攻撃がトラフィック異常性検知部10によって検知されると、シグネチャ生成部12は、検知対象のパケットの特徴を表すシグネチャを生成する。例えば、図3における攻撃検知条件の1番目の検知条件に合う攻撃が

検知された場合には、シグネチャ生成部12は、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であるパケットを示すシグネチャを生成する。

[0065] 上述した方法は、あらかじめ攻撃と判断するための条件を設定しておく方法であるが、平均的なトラフィックを測定して定常トラフィックとして記憶しておき、かかる定常トラフィックとの乖離から攻撃と判断する方法を用いることとしてもよい。

[0066] トラフィック異常性情報送信部11は、シグネチャ生成部12によって生成されたシグネチャを含み、トラフィックの異常性が検出されたことを表すトラフィック異常性情報を攻撃判断装置8に送信する処理部である。また、このトラフィック異常性情報送信部11は、自装置が正規な監視装置5であることを示す証明書を上記したトラフィック異常性情報に含めて送信する。このように、トラフィック異常性情報に証明書を含めることで、非正規な装置によるなりすましを防止することができる。

[0067] なお、トラフィック異常性情報送信部11は、パケットが送受信される伝送路6とは異なる経路でトラフィック異常性情報を送信するようにしてもよい。また、本実施例においては、トラフィック異常性情報を攻撃判断装置8に送信することとしたが、攻撃判断装置8が監視装置5のトラフィック異常性情報を参照するようにしてもよい。

[0068] 図1に示した性能測定装置7は、インターネットサイトの応答時間を測定するプログラムを実行するコンピュータによって構成されている。

[0069] 図4は、図1に示した性能測定装置7の構成を示すブロック図である。この性能測定装置7は、あらかじめ設定された性能異常性検知条件に基づいて性能の異常性を検出する性能異常性検知部16と、検出された性能異常性情報を攻撃判断装置8に送信する性能異常性情報送信部17と、攻撃判断装置8および性能を測定するための通信をそれぞれ行うための通信インタフェイス18、19とを備えている。

[0070] 図5は、性能異常性検知条件の一例を示す図である。図5において、性能異常性検知条件は、性能属性、検知閾値および検知回数の組からなる2組のレコードで構成される。性能属性は、性能を測定する手順を示し、検知閾値は、通信装置3からの応答時間の閾値を示し、検知回数は、測定回数と、測定回数のうち応答時間の閾値を上回った回数とを示している。

[0071] 例えば、1番目の性能異常性検知条件は、HTTPで、www.abc.comにアクセスし、"hello"れづ文字列が返ってくるまでの応答時間を測定するものである。そして、3回の測定のうち2回以上が5秒以上の応答時間であった場合に通信装置3の性能異常として検出する。

[0072] 同様に、2番目の性能異常性検知条件は、HTTPで、wwww.def.comにパラメータsearch?hl=ja&ie=UTF-8&q=x+Y&lr=”でアクセスし、“検索結果”という文字列が返ってくるまでの応答時間が1回でも5秒以上であった場合に通信装置3の性能異常として検出する。

[0073] このようにして、性能異常性検知部16が通信装置3の性能異常を検出すると、性能異常性情報送信部17は、性能の異常性が検出されたことを表す性能異常性情報を攻撃判断装置8に送信する。また、この性能異常性情報送信部17は、白装置が正規な性能測定装置7であることを示す証明書を上記した性能異常性情報に含めて送信する。このように、性能異常性情報に証明書を含めることで、非正規な装置によるなりすましを防止することができる。なお、本実施例においては、性能異常性情報を攻撃判断装置8に送信することとしたが、攻撃判断装置8が性能測定装置7の性能異常性情報を参照するようにしてもよい。

[0074] 上述した方法は、あらかじめ性能異常性を検出するための条件を設定しておく方法であるが、平均的な性能特性を測定して定常性能として記憶しておき、かかる定常性能との乖離から性能異常性を検出する方法を用いることとしてもよい。

[0075] 図6は、図1に示した攻撃判断装置8の構成を示すブロック図である。この攻撃判断装置8は、監視装置5から送られてきたトラフィック異常性情報と、性能測定装置7から送られてきた性能異常性情報とに基づいて、検出されたトラフィックの異常が、検出された性能異常を引き起こしているか否かを判断する影響判断部20と、判断結果をオペレータなどに通知するアラート送信部21と、監視装置5、性能測定装置7およびオペレータ通知用装置とそれぞれ通信を行うための通信インタフェイス22とを備えている。

[0076] 例えば、www.abc.comのホストアドレスが192.168.1.1であったとする。そして、ある時間tに、192.168.1.1宛のTCPポート番号が80のトラフィックが異常で

あることを表すトラフィック異常性情報を受け取り、続いて、時刻t＋αの時点でwww.abc.comの通信装置3のレスポンスタイム異常が発生したことを表す性能異常性情報を受け取ったとする。このような状況において、各異常性情報に係る異常が発生した時間が近い場合（例えばαが1分以内）には、トラフィックの異常性がwww.abc.comのレスポンス悪化を引き起こしている可能性が高いと判断し、アラート送信部21を通してオペレータにその旨を伝え対処を促す。

[0077] このようにして、影響判断部20がサービス不能攻撃であると判断すると、アラート送信部21は、かかる判断に用いたトラフィック異常性情報および性能異常性情報をオペレータ通知用装置に送信する。なお、本実施例においては、かかるトラフィック異常性情報および性能異常性情報をオペレータ通知用装置に送信することとしたが、攻撃判断装置8が表示装置などを備えることによりこれらの異常性情報をオペレータに通知するようにしてもよい。

[0078] また、かかる影響判断部20は、監視装置5から送られてきたトラフィック異常性情報および性能測定装置7から送られてきた性能異常性情報に含まれる証明書に基づいた認証をおこなったうえで、サービス不能攻撃であるか否かを判断することとしてもよい。このようにすることで、偽造されたトラフィック異常性情報や性能異常性情報による影響を排除することができる。

[0079] 以上のように構成されたサービス不能攻撃検知システム1について、図7～図9を用いてその動作を説明する。図7は、図2に示した監視装置5の動作を示すフローチャートである。

[0080] まず、通信機器3に送信されるパケットによる攻撃がトラフィック異常性検知部10によって攻撃検知条件に基づいて検知されると（ステップS1）、攻撃が検知されたパケットの特徴を表すシグネチャがシグネチャ生成部12によって生成され（ステップS2）、生成されたシグネチャを含むトラフィック異常性情報が異常性情報送信部111によって攻撃判断装置8に送信される（ステップS3）。

[0081] 図8は、図4に示した性能測定装置7の動作を示すフローチャートである。まず、性能異常性検知部16によって性能異常検知条件に基づいて通信機器3の応答時間の異常性が検知されると（ステップS11）、検知された情報を含む性能異常性情報を

生成し(ステップS12)、生成された性能異常性情報が性能異常性情報送信部17によって攻撃判断装置8に送信される(ステップS13)。

[0082] 図9は、図6に示した攻撃判断装置8の動作を示すフローチャートである。監視装置5からトラフィック異常性情報が送られてくると(ステップS21)、それまでに受け取っている性能異常性情報の中から、そのトラフィック異常性が原因になっていると思われるものを検索し(ステップS22)、見つかった場合にはかかるトラフィック異常性情報および性能異常性情報をオペレータ通知用装置に送信する(ステップS23)。

[0083] また、性能測定装置7から性能異常性情報が送られてきた場合には(ステップS24)、それまでに受け取っているトラフィック異常性情報の中から、その性能異常性の原因になっていると思われるものを検索し(ステップS25)、見つかった場合にはかかるトラフィック異常性情報および性能異常性情報をオペレータ通知用装置に送信する(ステップS23)。

[0084] 上述してきたように、サービス不能攻撃検知システム1によれば、トラフィック異常性および性能異常性を検知して、これらの異常性の関連を判断することにより、性能異常を引き起こしているトラフィック異常のみを検出することができるので、サービス不能攻撃の検知精度を向上させることによって運用者の対処を必要とするサービス不能攻撃のみを検出することができる。

[0085] なお、上記実施例に示した監視装置、性能測定装置および攻撃判断装置は、コンピュータにプログラムをロードして実行することにより機能発揮する。具体的には、監視装置のコンピュータのROM(ReadOnlyMemory)等に通信機器宛パケットのトラフィック異常性を検知するルーチンを含むプログラムを記憶し、また、性能測定装置のコンピュータのROM等に通信機器の性能異常性を検知するルーチンを含むプログラムを記憶し、また、攻撃判断装置のコンピュータのROM等にトラフィック異常性情報および性能異常性情報の関連を判断するルーチンを含むプログラムを記憶しておき、各装置がこれらのプログラムをCPUにロードして実行することにより、本発明に係る監視装置、性能測定装置および攻撃判断装置を形成することができる。

産業上の利用可能性

[0086] 以上のように、本発明にかかるサービス不能攻撃検知システムおよびサービス不能

攻撃検知方法は、通信機器へのサービス不能攻撃を検知する場合に適している。

請求の範囲

[1] サービス不能攻撃対象となる通信機器宛に送信されたパケットを監視する監視装置と、前記通信機器の性能を測定する性能測定装置と、前記監視装置および前記性能測定装置と通信をおこなう攻撃判断装置とによって前記通信機器に対するサービス不能攻撃を検知するサービス不能攻撃検知システムであって、

前記監視装置は、

前記通信機器に対する前記パケットによるトラフィックの異常性を表すトラフィック異常性情報を検知するトラフィック異常性検知手段

を備え、

前記性能測定装置は、

前記通信機器の処理能力の異常性を表す性能異常性情報を検知する性能異常性検知手段

を備え、

前記攻撃判断装置は、

前記トラフィック異常性情報および前記性能異常性情報に基づいてサービス不能攻撃であるか否かを判断する影響判断手段

を備えたことを特徴とするサービス不能攻撃検知システム。

[2] 前記監視装置は、前記トラフィック異常性情報を前記攻撃判断装置に送信するトラフィック異常性情報送信手段をさらに備えたことを特徴とする請求項1に記載のサービス不能攻撃検知システム。

[3] 前記性能測定装置は、前記性能異常性情報を前記攻撃判断装置に送信する性能異常性情報送信手段をさらに備えたことを特徴とする請求項1または2に記載のサービス不能攻撃検知システム。

[4] 前記トラフィック異常性検知手段は、あらかじめ設定された所定の攻撃検知条件に基づいて前記トラフィック異常性情報を検知することを特徴とする請求項1に記載のサービス不能攻撃検知システム。

[5] 前記トラフィック異常性検知手段は、前記攻撃検知条件に基づいて前記通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを生成し、前記シグネチャを

含む前記トラフィック異常性情報を生成することを特徴とする請求項4に記載のサービス不能攻撃検知システム。

[6] 前記トラフィック異常性検知手段は、前記通信機器宛の前記パケットの平均的なトラフィックを表す定常トラフィックに基づいて前記トラフィック異常性情報を検知することを特徴とする請求項1に記載のサービス不能攻撃検知システム。

[7] 前記性能異常性検知手段は、あらかじめ設定された所定の性能異常性検知条件に基づいて前記性能異常性情報を検知することを特徴とする請求項1に記載のサービス不能攻撃検知システム。

[8] 前記性能異常性検知条件は、前記通信機器に応答要求メッセージを送信してから前記応答要求メッセージに対応する応答メッセージを受信するまでの応答時間と、前記応答時間が所定の閾値を上回る回数とを含んだことを特徴とする請求項7に記載のサービス不能攻撃検知システム。

[9] 前記性能異常性検知手段は、前記通信機器の平均的な性能特性を表す定常性能に基づいて前記性能異常性情報を検知することを特徴とする請求項1に記載のサービス不能攻撃検知システム。

[10] 前記影響判断手段は、前記トラフィック異常性情報および前記性能異常性情報に含まれる異常発生時刻に基づいて該トラフィック異常性情報または該性能異常性情報のいずれか一方の異常性情報に起因して他方の異常性情報が発生したと判断した場合にサービス不能攻撃であると判断することを特徴とする請求項1に記載のサービス不能攻撃検知システム。

[11] 前記影響判断手段がサービス不能攻撃であると判断した場合に、該判断に用いた前記トラフィック異常性情報および前記性能異常性情報を前記攻撃判断装置がオペレータ通知用装置に送信することを特徴とする請求項1に記載のサービス不能攻撃検知システム。

[12] 前記影響判断手段は、前記トラフィック異常性情報および前記性能異常性情報に含まれる証明書に基づいた認証を行ったうえで、サービス不能攻撃であるか否かを判断することを特徴とする請求項1に記載のサービス不能攻撃検知システム。

[13] サービス不能攻撃対象となる通信機器宛に送信されたパケットを監視する監視装

置と、前記通信機器の性能を測定する性能測定装置と、前記監視装置および前記性能測定装置と通信をおこなう攻撃判断装置とによって前記通信機器に対するサービス不能攻撃を検知するサービス不能攻撃検知方法であって、

前記通信機器に対する前記パケットによるトラフィックの異常性を表すトラフィック異常性情報を前記監視装置が検知するトラフィック異常性検知工程と、

前記通信機器の処理能力の異常性を表す性能異常性情報を前記性能測定装置が検知する性能異常性検知工程と、

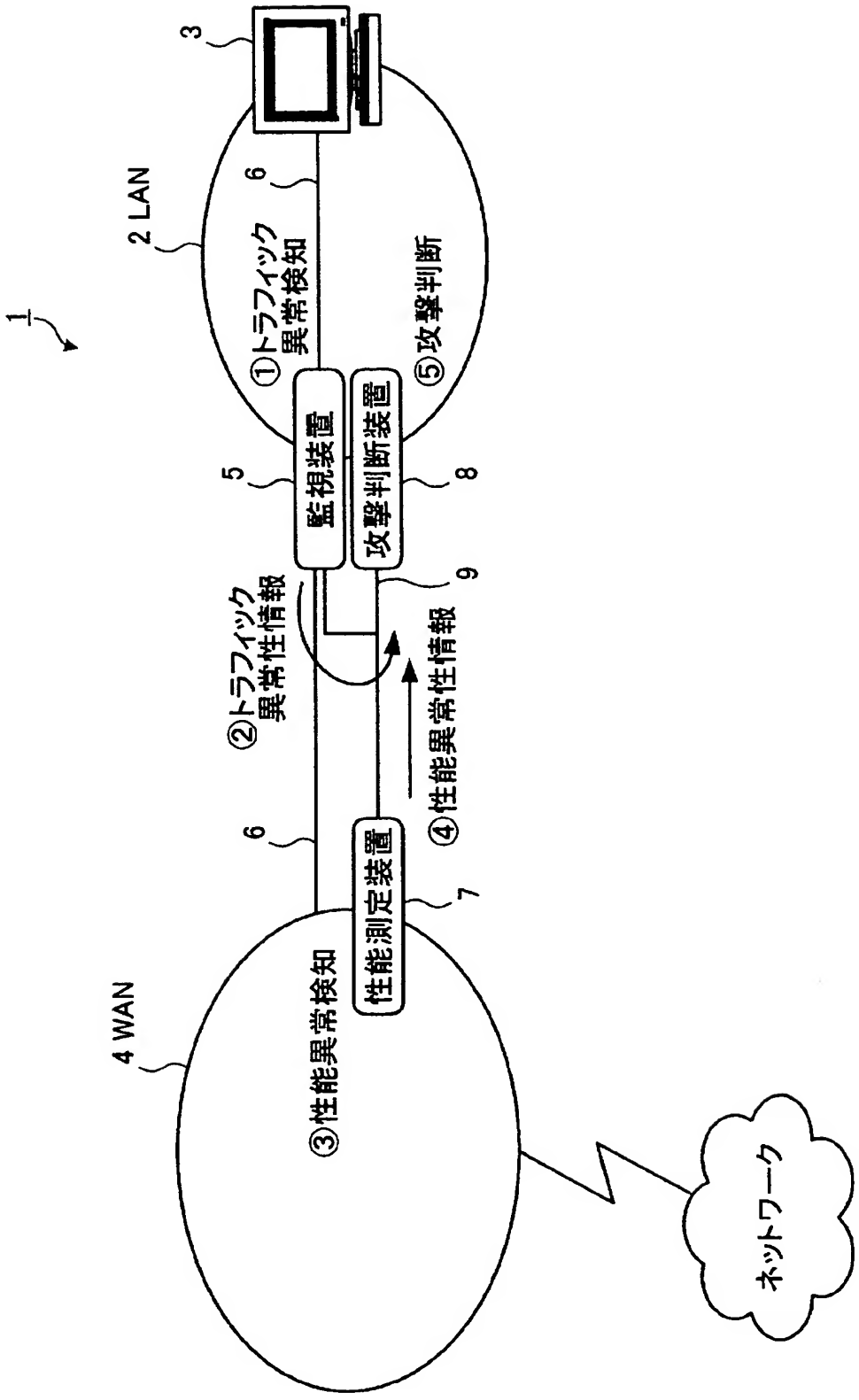
前記トラフィック異常性情報および前記性能異常性情報に基づいてサービス不能攻撃であるか否かを前記攻撃判断装置が判断する影響判断工程と

を含んだことを特徴とするサービス不能攻撃検知方法。

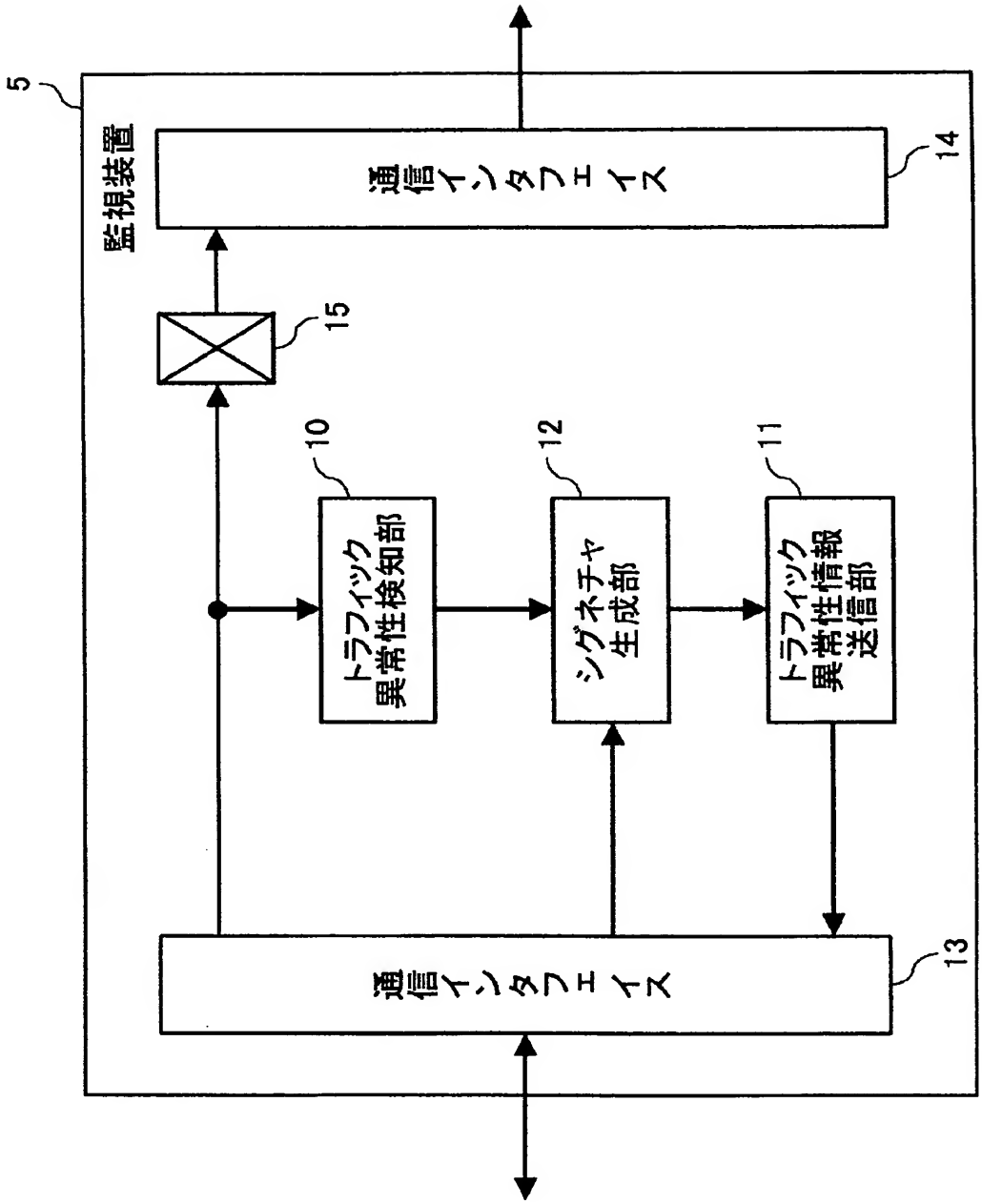
[14] 前記トラフィック異常性情報を前記監視装置が前記攻撃判断装置に送信するトラフィック異常性情報送信工程をさらに含んだことを特徴とする請求項13に記載のサービス不能攻撃検知方法。

[15] 前記性能異常性情報を前記性能測定装置が前記攻撃判断装置に送信する性能異常性情報送信工程をさらに含んだことを特徴とする請求項13または14に記載のサービス不能攻撃検知方法。

[図1]


1
2 LAN
3
4 WAN
5
6
7
8
9
①トラフィック異常検知
②トラフィック異常性情報
③性能異常検知
④性能異常性情報
⑤攻撃判断
監視装置
攻撃判断装置
性能測定装置
ネットワーク

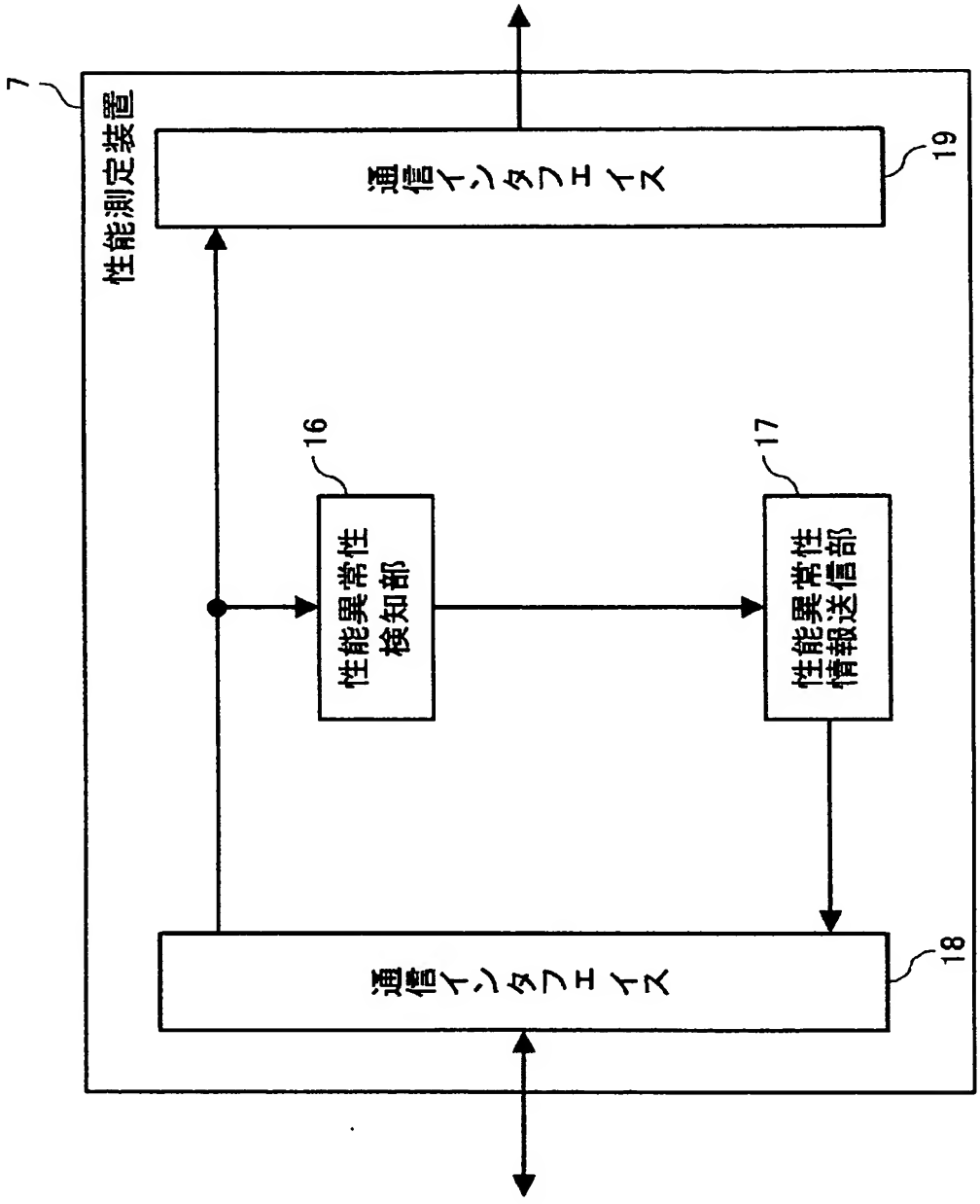
[図2]


5
監視装置
通信インタフェース
14
15
10
トラフィック異常性検知部
12
シグネチャ生成部
11
トラフィック異常性情報送信部
通信インタフェース
13

[図3]

	検知属性	検知閾値	検出時間
1	{Dst=192.168.1.1/32, Protocol=TCP, Port=80}	300kbps	10秒
2	{Dst=192.168.1.2/32}	100kbps	10秒

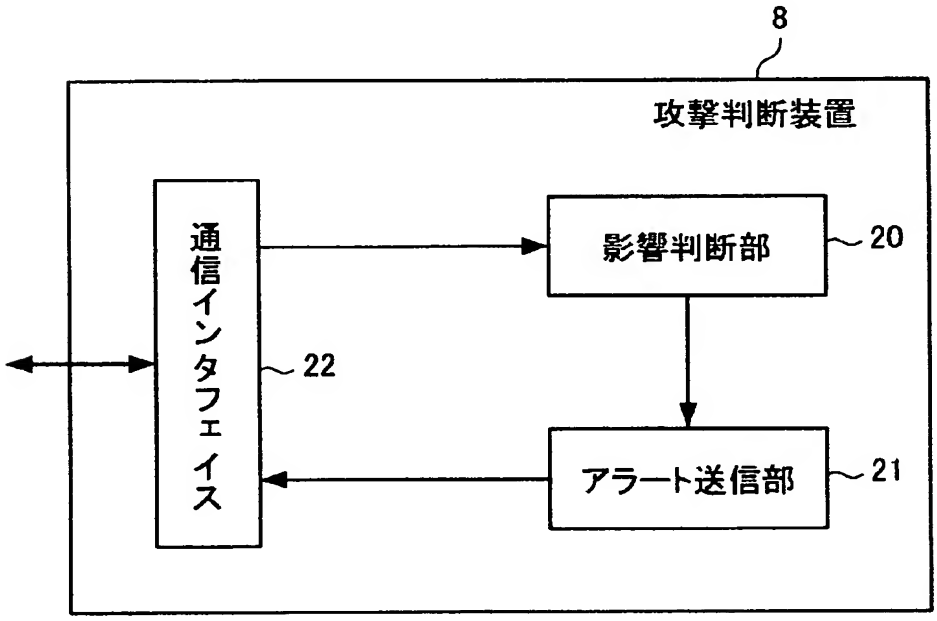
[図4]


7
性能測定装置
通信インタフェース
19
16
性能異常性検知部
17
性能異常性情報送信部
通信インタフェース
18

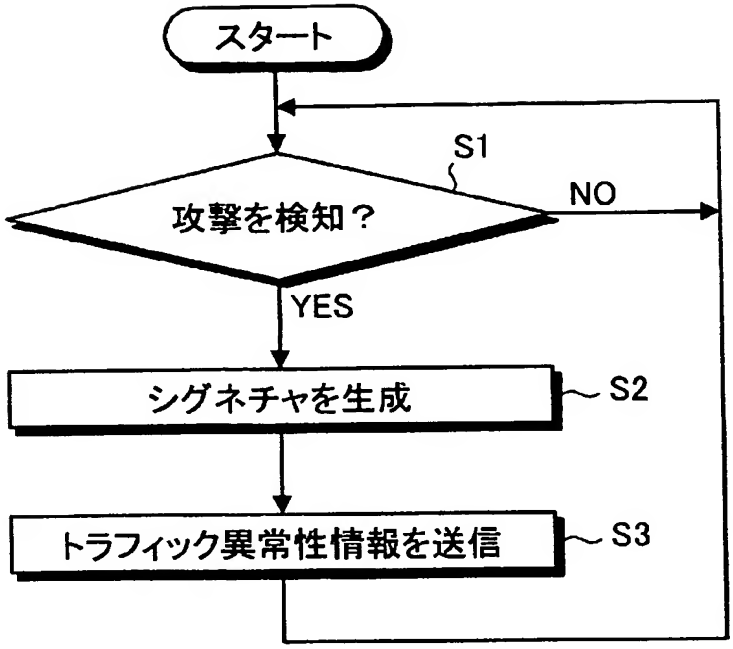
[図5]

	性能属性	検知閾値	検出回数
1	{Dst=http://www.abc.com} {res="hello"}	5秒	2/3
2	{Dst=http://www.def.com/serch?hl=ja&ie=UTF-8&q=x+Y&lr=} {res="検索結果"}	5秒	1/1

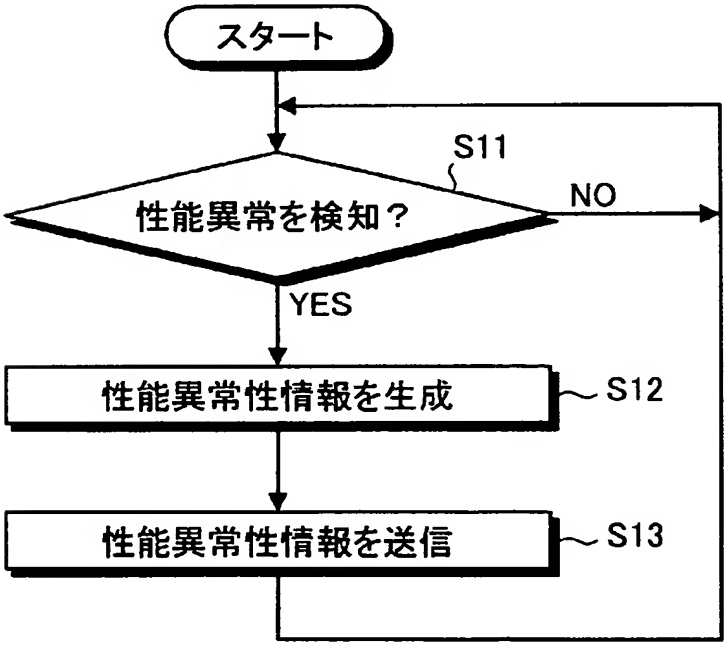
[図6]



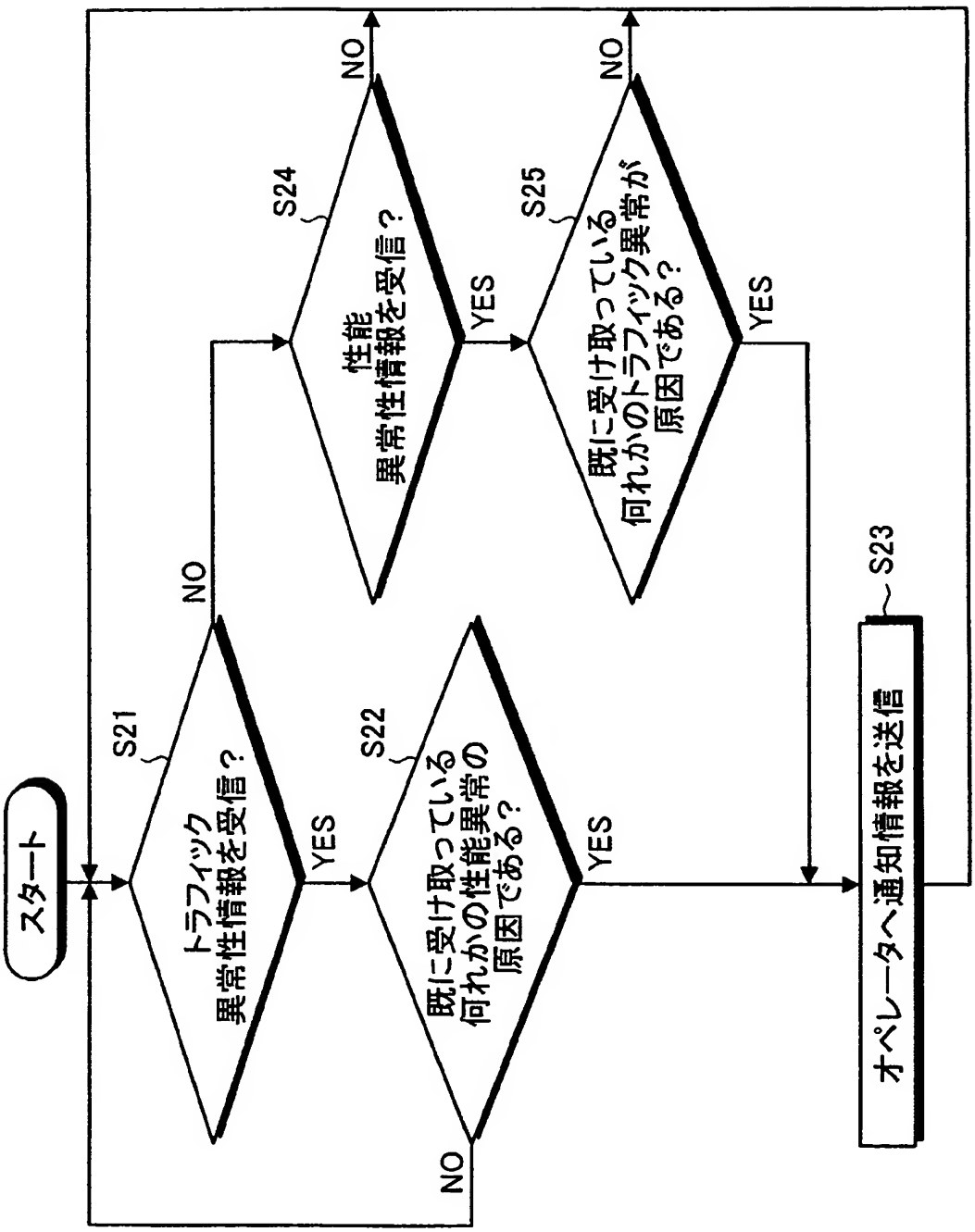
[図7]


スタート
S1
攻撃を検知？
NO
YES
シグネチャを生成
S2
トラフィック異常性情報を送信
S3

[図8]


スタート
S11
性能異常を検知？
NO
YES
性能異常性情報を生成
S12
性能異常性情報を送信
S13

[図9]


スタート
S21
トラフィック
異常性情報を受信？
YES
NO
S22
既に受け取っている
何れかの性能異常の
原因である？
YES
NO
S24
性能
異常性情報を受信？
YES
NO
S25
既に受け取っている
何れかのトラフィック異常が
原因である？
YES
NO
S23
オペレータへ通知情報を送信

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/015156

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/66(2006 .01) , ***H04L12/56*** (2006 .01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/66(2006 .01) , ***H04L12/56*** (2006 .01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-164553 A (Toshiba Corp.), 10 June, 2004 (10.06.04), Par. Nos. [0027] to [0047], [0091] & US 2004/0064738 A1	1-15
Y	JP 2003-283555 A (Nippon Telegraph And Telephone Corp.), 03 October, 2003 (03.10.03), Claim 1; Figs. 1 to 11 (Family: none)	1-15
Y	JP 2004-280724 A (Fujitsu Ltd.), 07 October, 2004 (07.10.04), Par. Nos. [0042], [0154] to [0157] & US 2004/0187034 A1	12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 November, 2005 (24.11.05)	06 December, 2005 (06.12.05)
Name and mailing address of the ISA/ Japanese Patent Office	A thonzed officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

国際調査報告

国際出願番号 PCTノJP2005/ 015156

A． 発明の属する分野の分類 (国際特許分類 (ｉＰＣ))
Int.Cl. *H04L12/66* (2006.01), 旺oA几72/56(2006.01)

B． 調査を行った分野

調査を行った最小限資料 (国際特許分類 (ＩＰＣ))
Int.Cl. ***HOA乙12/66*** (2006.01), ***HOAじ12/56(2006.01)***

小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２- １９９６年
日本国公開実用新案公報	１９７１—２００５年
日本国実用新案登録公報	１９９６- ２００５午
日本国登録実用新案公報	１９９４- ２００５年

国際調査で使用した電子データベース (データベースの名称 •調査に使用した用語)

C． 関連すると認められる文献

引用文献のカテゴリーホ	引用文献名 及び一部の箇所が関連するとき泣、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2004-164553 A (株式会社東芝) 2004. 06. 10, 段落 [0027]-[0047], [0091] & US 2004/0064738 Al	1-15
Y	JP 2003-283555 A (日本電信電話株式会社) 2003. 10. 03, 請求項 1, 図 1-ii (ファミリーなし)	1-15
Y	JP 2004-280724 A (富士通株式会社) 2004. 10. 07, 段落 [0042], [0154]-[0157] & us 2004/0187034 Al	12

頂 C欄の続きにも文献が列挙されている。

匚 パテントﾌｧﾐﾘｰに関する別紙を参照。

ホ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しく肚他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献.
rpj 国際出願日前で、かつ優先権の主張の基礎となる出願の目の役に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願t矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であつて、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当謙文献t他の1以上の文献≧の、当業者にとって自明である組合せによって進歩性がないと考えられるもの
r&j 同一パテントyァミリ—文献

国際調査を完Tした日 24. 11. 2005	国際調査報告の発送日 06. 12. 2005
国際調査機関の名称及びあて先 日本国特許庁 (ＩＳＡ/ ＪＰ) 郵便番号１００- ８９１５ 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 5X 9851 寺谷 大亮 電話番号 03- 3581- 1101 内線 3596

様式PCT ノISAノ210 第2ページ) (2005年4月)